

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

RIBEIRO TRELHA GUSTAVO
a/k/a Matos Fontinele,

Defendant.

CASE NO. CR17-190 RSL

**GOVERNMENT'S SENTENCING
MEMORANDUM**

Sentencing Hearing: Dec. 15, 2017

I. INTRODUCTION AND SENTENCING RECOMMENDATION

Defendant RIBEIRO TRELHA GUSTAVO is before the Court to be sentenced for stealing bank account information from hundreds of unsuspecting victims. In April 2017, Gustavo used skimming devices and video cameras attached to an ATM to surreptitiously collect the account and PIN numbers of ATM users and record their personal financial information so he or his associates could fraudulently access their bank accounts. In the three days Gustavo was observed skimming at a single ATM in Seattle, nearly 300 account numbers were compromised.

1 Defendant's theft does more than financially harm banks and their customers,
2 schemes like his impose substantial costs on victimized account holders' time and, more
3 importantly, sense of security. The United States recommends Defendant be sentenced to a
4 term of imprisonment of twelve months and one day, followed by three years of supervised
5 release. This sentence is necessary to reflect the seriousness of the offense, impose just
6 punishment, and deter future fraud by Defendant and those who would follow his example.
7

8 **II. BACKGROUND**

9 As described below, Defendant used a credit card "skimming" device and an
10 electronic camera on Automatic Teller Machines (ATMs) to secretly steal the credit and
11 debit card numbers of the ATM users and record the entry of their personal identification
12 numbers (PIN) as they used the machine.

13 Beginning at a time unknown, but no later than April 25, 2017 and continuing
14 through April 27, 2017, Defendant installed a fraudulent bank card skimming device
15 along with an electronic camera capable of capturing the customer/victim's bank card
16 and PIN at a JPMorgan Chase ATM in downtown Seattle. This activity was detected
17 by bank investigators. According to JPMorgan Chase, 292 accounts were
18 compromised from that single ATM during the three days Defendant's skimming
19 activity was identified. It is unknown how many additional accounts were
20 compromised through Defendant's skimming activity, or the loss suffered as a result.
21

22 On April 27, 2017, after the skimming activity was detected, Defendant was
23 arrested at the scene of the ATM, which law enforcement found rigged with a
24 skimming device and a modified ATM camera to record entry of PIN numbers. On
25 his person at the time of the arrest, Defendant had ten fraudulent cards and a Brazilian
26 identification card bearing Defendant's picture and the alias Matos Fontinele. Seven
27 of the bank cards embossed with the name of Fontinele and an embossed bank card
28

number had been produced or altered so that the card numbers encoded on the magnetic stripe that were different from those embossed on the front of the bank card.

In a search of Defendant's hotel room the following day, law enforcement found, among other things: three more modified ATM cameras and an additional ATM skimmer, a credit card reader/writer, numerous blank credit cards, and other tools consistent with improvising and building additional devices and attaching those devices to ATMs, such as super glue, scissors, and double-stick tape.

Law enforcement also recovered various electronic media including three hard drives, a laptop, and several SD cards. Search of that media revealed at least 62 credit card numbers in the text files, as well as hundreds of photo and video clips from the ATM cameras of PIN numbers being entered.

Defendant told law enforcement that he would nightly upload the skimmed account numbers to the "cloud," to be retrieved and downloaded by co-conspirators in Brazil. Accordingly, the 62 account numbers recovered (and used to determine the loss amount) likely far underestimate the scope of the fraud, including the number of accounts skimmed and account holders victimized, and the loss amount resulting from the theft.¹

III. THE ADVISORY GUIDELINES RANGE

The government agrees with Probation's guideline calculation, which is as follows:

<u>Adjustment</u>	<u>Calculation</u>	<u>Provision</u>
Base Offense Level	+6	2B1.1
Loss Exceeding \$15,000	+4	2B1.1(b)(1)(C)
More than 10 Victims	+2	2B1.1(b)(2)(A)
Use of Sophisticated Means	+2	2B1.1(b)(10)(C)
Use of Device-Making Equipment	+2	2B1.1(b)(11)(A)(i)
Acceptance of Responsibility	-3	3E1.1(b)
Total Offense Level:	13	

¹ Law enforcement was unable to determine a restitution amount from Chase or other victim banks and their customers. Accordingly, the government is not seeking restitution as part of the sentence, despite Defendant's agreement to pay restitution in an amount to be determined at or before sentencing.

1 Defendant's Criminal History Category is I, resulting in a guideline range of **12-18**
2 months.
3

4 **IV. RATIONALE FOR SENTENCING RECOMMENDATION**

5 The United States recommends that Defendant be sentenced to a term of
6 imprisonment of twelve months and one day, to be followed by three years of supervised
7 release.² This sentence is sufficient, but not greater than necessary to comply with the
8 following factors set out in 18 U.S.C. § 3553(a):

9 **A. Nature and Circumstances of the Offenses**

10 There are several aggravating factors involved in Defendant's theft. First, its
11 repetition and breadth suggest that the discovered conduct may be merely the tip of an
12 iceberg of fraud. As noted, Chase bank was able to identify 292 compromised accounts
13 based on only three days of activity. Hotel and vehicle rental information suggest that
14 Defendant had been in Washington for roughly a week before that three-day period began.
15 And, evidence linking fraudulent activity to Florida (from where Defendant apparently came
16 to Washington) shows the fraud activity was not limited to this jurisdiction.³ All told, there
17 is a pattern of repeated conduct, each incident of which constitutes a separate crime
18 victimizing banks and their customers. Unfortunately, law enforcement has not been able to
19 determine the extent of loss or restitution, but that fact should not obscure the true nature of
20 Defendant's fraud.
21
22
23

24
25 ² The government agreed to recommend a custodial term no higher than the low-end of the advisory
26 guidelines range, anticipated to be 12 months. Defendant requested that, assuming the calculation is correct,
the government cap its recommendation at 12 months and one day, which the government agreed to do.

27 ³ Defendant had in his hotel room a temporary Florida identification card, and a FedEx label in his car
28 showing materials sent from Winter Park, Florida to the hotel room where he was staying in Seattle. A
receipt in his possession showed a cash deposit of \$5060.00 in Orlando, Florida on April 4, 2017, and
transaction activity related to the accounts recovered on his computer include significant activity in Florida.

1 Second, the nature of identity theft and related crimes stands as an aggravating factor.
2 Even where, as here, banks appear to have borne or mitigated the financial loss, that fact
3 does little to heal the loss of peace of mind that results from theft of victims' personal
4 information. This increasingly common experience is at best frustrating and at worst
5 terrifying for the millions who endure it, and the consequences are very real. In 2012, an
6 estimated 16.6 million people in the United States experienced at least one incident of
7 identity theft. *See Bureau of Justice Statistics*,
8 <http://www.bjs.gov/content/pub/press/vit12pr.cfm>. The financial costs of identity theft were
9 estimated at \$24.7 billion for that year alone. *Id.* This staggering figure was \$10 billion
10 more than the losses attributed to all other property crimes. *Id.* The misuse of their personal
11 information drags the unwitting individuals involved in this offense into the middle of a
12 broader problem, a problem that Defendant's actions helped perpetuate.

13
14 Third, his deception was notable for its forethought and sophistication. Defendant, or
15 his associates, fashioned devices to mimic the appearance and function of an ATM card
16 reader and camera in order to steal without detection. He used, according to his own
17 statements, a computer program to transfer the stolen account information to associates
18 outside the United States. He carried identification and credit cards in a false name to
19 conceal his identity. And, according to travel and vehicle rental information, he traveled
20 from Florida to Washington to execute the scheme. Unfortunately, the steps defendant took
21 to conceal his scheme and evade detection were effective to a large extent, and the
22 government has been mainly unable to determine how many accounts may have been
23 compromised by Defendant, and the resulting loss to banks and customers.⁴

24
25
26 ⁴ Defendant is expected to claim that he was a small player in this operation, and previously told law
27 enforcement he earned \$100 per day for his skimming activity. The government has been unable to verify
28 that claim, but noted that he had in his possession bank deposit slips totaling close to \$6,000 when arrested.
According to the report of the United States Probation Office, Defendant maintained a construction company
with his girlfriend that earned, for the pair, somewhere between \$1500 (PSR ¶ 55) and \$3000 (*Id.* ¶ 56) per

1 Finally, Defendant's conduct plainly satisfies the elements of Aggravated Identity
2 Theft, as Defendant's access device fraud scheme depended on the theft of victims' personal
3 identifying information. Though the government chose not to bring that charge, the fact that
4 this very same conduct carries a mandatory two-year consecutive sentence is relevant for
5 sentencing purposes.
6

7 **B. Defendant's History and Characteristics**

8 Defendant's history and circumstances provide no justification for his offense. As
9 described by the U.S. Probation Office, Defendant was raised in an intact home by loving
10 parents, is educated, and has a history of consistent and productive employment. According
11 to Defendant, he came to the United States to pursue legitimate business interests before
12 overstaying his visa and turning to fraud. He has no addictions or other compulsions that
13 sometimes accompany fraud conduct, nor any mental health challenges. There is nothing in
14 that background to explain his criminal conduct or provide context for his decision to
15 victimize unsuspecting ATM users, other than simple greed.
16

17 Defendant appears to have a supportive family in Brazil, including a four-year-old
18 son. While these ties, paired with his lack of a prior criminal record, may be viewed as
19 mitigating factors, they also underscore the senseless nature of his conduct, and call into
20 question the claim that Defendant would risk prosecution and incarceration in a foreign
21 country for a purported \$100 a day.
22

23 **C. Other Sentencing Factors**

24 A significant term of imprisonment is necessary to reflect the seriousness of the
25 offense, impose just punishment, and to provide deterrence. Based on the observed pace of
26 Defendant's skimming activities, his conduct had the potential to – if it did not already –
27
28 week. He also reported savings of \$125,000 in Brazil (*Id.* ¶ 58). This relative financial security begs the
question of why defendant would engage in this criminal activity for a claimed \$100 per day.

1 victimize thousands of individuals who did no more than use an ATM. While Chase
2 promptly notified those whose accounts were breached, they nonetheless endured the burden
3 of reviewing their transaction history, reporting suspicious activity, and changing any
4 automatic payments to a new card. More importantly, victims were left with the uncertainty
5 and attendant anxiety of not knowing whether their personal financial information is safe and
6 protected.
7

8 The recommended sentence – as well as the likely immigration consequences that will
9 result – would also deter others who would contribute to the plague of identity theft
10 occurring in this country, which not only harms its victims but also drains critical resources
11 to investigate and eradicate fraud.

12 **V. CONCLUSION**

13 For the reasons described above, the United States recommends that Defendant be
14 sentenced to a term of imprisonment of twelve months and one day, to be followed by three
15 years of supervised release.
16

17 Dated: December 8, 2017

18 Respectfully submitted,

19
20 ANNETTE L. HAYES
21 United States Attorney

22 /s/ Benjamin T. Diggs
23 BENJAMIN T. DIGGS
24 Special Assistant United States Attorney
25 United States Attorney's Office
26 700 Stewart Street, Suite 5220
27 Seattle, Washington 98101-1271
28 Phone: 206-553-7970
E-mail: benjamin.diggs@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on December 8, 2017, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant(s).

/s/Dru Mercer

DRU MERCER

Paralegal

United States Attorney's Office

700 Stewart Street, Suite 5220

Seattle, Washington 98101-1271

Telephone: (206) 553-7970

Facsimile: (206) 553-2502